PCT

(51) International Patent Classification 5 : **G06F 1/02**	**A1**	(11) International Publication Number: **WO 95/06906** (43) International Publication Date: 9 March 1995 (09.03.95)

(21) International Application Number: PCT/US94/07774

(22) International Filing Date: 11 July 1994 (11.07.94)

(30) Priority Data:
08/114,804   30 August 1993 (30.08.93)   US

(71) Applicant: MOTOROLA INC. [US/US]; 1303 East Algonquin Road, Schaumburg, IL 60196 (US).

(72) Inventors: PUHL, Larry, C.; 6 Plum Court, Sleepy Hollow, IL 60118 (US). FINKELSTEIN, Louis, David; 1698 W. Ottowa Court, Wheeling, IL 60090 (US).

(74) Agents: PARMELEE, Steven, G. et al.; Motorola Inc., Intellectual Property Dept./KAB, 1303 East Algonquin Road, Schaumburg, IL 60196 (US).

(81) Designated States: BR, CA, FI, GB, JP, KR, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(54) Title: METHOD AND APPARATUS FOR ENCRYPTION HAVING A FEEDBACK REGISTER WITH SELECTABLE TAPS
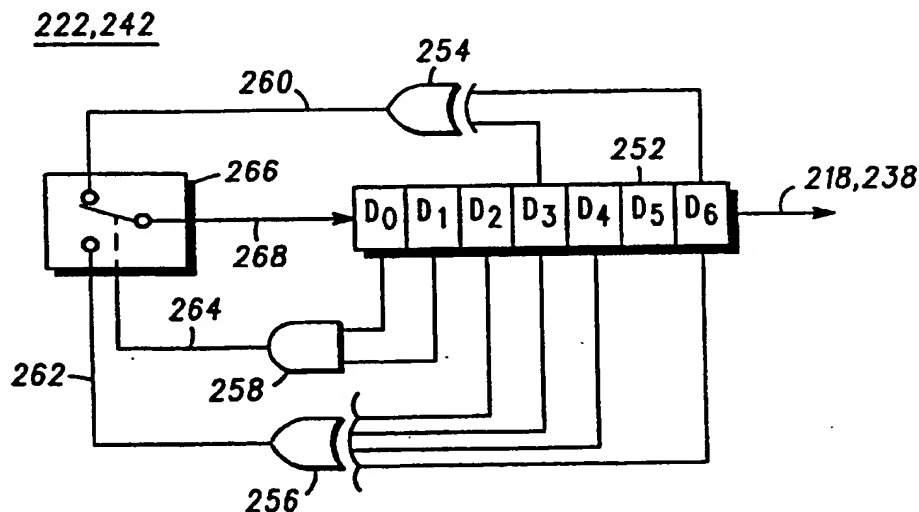
(57) Abstract

A method and apparatus for generating a pseudo-random bit sequence is provided. A first input bit (260) is determined as a function of bits stored in a shift register (252) in accordance with a first feedback algorithm. In addition, a second input bit (262) is determined as a function of bits stored in the shift register (252) in accordance with a second feedback algorithm. Subsequently, a particular input bit (268) to be provided to the shift register (252) is deterministically selected from the group consisting of the first input bit (260) and the second input bit (262) such that a non-linear pseudo-random sequence may be produced by the shift register (252). In addition, a communication unit which utilizes the pseudo-random bit sequence in encrypting a signal to be transmitted and decrypting a received signal is described.

-1-

METHOD AND APPARATUS FOR ENCRYPTION HAVING A FEEDBACK REGISTER WITH SELECTABLE TAPS

Field of the Invention

5

The present invention relates to communication systems and, more particularly, to encryption within communication systems in which a feedback register output is used as an encryption variable. This feedback register includes selectable taps to protect it from

10   cryptographic attack.

Background of the Invention

Many communications systems currently use encryption to

15   enhance security of the systems. These communication systems include but are not limited to cellular radio telephone communication system, personal communication systems, paging systems, as well as wireline and wireless data networks. By way of example a cellular communication system will be described below; however, it will be

20   appreciated by those skilled in the art that the encryption techniques described can be readily extended to other communication systems without departing from the scope and spirit of the present invention.

Turning now to cellular communication systems, these systems typically include subscriber units (such as mobile or portable units)

25   which communicate with a fixed network communication unit via radio

-2-

frequency (RF) communication links. In cellular communication systems, the RF communication link is the primary target for cryptographic systems, because it is the most vulnerable to unauthorized introduction (spoofing) or extraction (eavesdropping) of information. It is well known

5   in the art that information in these communication links may be cryptographically protected by encrypting them with a pseudo-noise (PN) signal which is pseudo-random in nature. For example this may be accomplished by performing an exclusive-or operation of an information signal with a PN signal, prior to transmission. Subsequently, the inverse

10   operation can be performed during the receiving process.

The PN signals are not truly random, but appear random when subject to cursory inspection. The advantage of these PN signals is that they can be easily generated by a linear feedback shift register (LFSR). An LFSR generates a PN signal which is periodic (i.e., deterministic).

15   The periodicity of the PN signal is dependent on the number of stages (i.e., bits stored) in the register, the feedback "taps", and the initial state of the LFSR stages. The LFSR implements an Nth degree polynomial (where N is the number of stages of the LFSR) by having one feedback signal "tap" (output bit of a stage) for each coefficient of the polynomial.

20   An input bit is formed from an exclusive-or operation on the outputs of these feedback signal "taps" and feed back into the register. Ideally feedback "taps" can be chosen which implement a maximal length PN signal generator. A maximal length PN generator generates a pseudo random sequence which repeats every 2^N-1 cycles, where N is the

25   number of stages in the in the register. Examples of maximal length feedback tap arrangements for several different stage length registers are given in "Error-Correcting Codes", second edition by W. Wesley Peterson and E.J. Weldon, Jr., MIT Press, 1972.

The problem with using PN generators to cryptographically

30   protect an information signal is that they are extremely vulnerable to attack (i.e., the encryption is easy to crack or break). The weakness of PN generators which are based on an LFSR is primarily due to the inherent linearity of the generators. Since PN generators operate according to an algorithm, knowledge of the algorithm reveals the entire

35   sequence. Further, as noted in chapter 5 of "Cipher Systems" by Henry Baker and Fred Piper, Northwood Publications, 1992, a cryptoanalyst needs only 2N bits of plaintext and corresponding ciphertext for an N

-3-

stage long LFSR to be able to determine the feedback "taps", the initial
state of the LFSR, and ultimately any PN signal output by the LFSR.
This vulnerability represents a major drawback to the continued use of
the LFSR to cryptographically protect communication systems.

5   Therefore, a need exists for a cryptographically protection
technique for communication systems which can alleviate these
problems.

Summary of the Invention

10

A method and apparatus for generating a pseudo-random bit
sequence is provided. A first input bit is determined as a function of bits
stored in a shift register in accordance with a first feedback algorithm. In
addition, a second input bit is determined as a function of bits stored in
15   the shift register in accordance with a second feedback algorithm.
Subsequently, a particular input bit to be provided to the shift register is
deterministically selected from the group consisting of the first input bit
and the second input bit such that a non-linear pseudo random
sequence may be produced by the shift register. In addition, a
20   communication unit which utilizes the pseudo-random bit sequence in
encrypting a signal to be transmitted and decrypting a received signal is
described.

Brief Description of the Drawings

25

FIG. 1 is a block diagram showing a preferred embodiment
cryptographic process for use in a communication system having a
subscriber unit and a fixed network communication unit in accordance
with the present invention.
30   FIG. 2 is a block diagram of a preferred embodiment pseudo-
random bit sequence generator to be used by either a subscriber unit or
a fixed network communication unit shown in FIG. 1 in accordance with
the present invention.

-4-

Detailed Description

Referring now to FIG. 1, a preferred embodiment cryptographic process for use in a communication system having a subscriber communication unit **202** and a fixed network communication unit **200** (i.e., cellular base site) in accordance with the present invention is shown. The fixed network communication unit **200** is connected to other parts of the fixed network through a base site controller **210** by a coupler **212**. The other parts of the fixed network may include, but are not limited to, other communication units, central controllers, communication system switches, or an access port on the public switched telephone network (PSTN). In operation, an information signal (i.e., a voice and/or data signal) is input to the communication system from either the fixed network (via coupler **212**) or from other parts of the subscriber communication unit **202**. Subsequently, the information signal is encrypted and transmitted over the communication channel **204**, as well as received and decrypted by communication unit which did not transmit the information signal (i.e., either the fixed network communication unit **200** or the subscriber communication unit **202**, respectively).

By way of example, the communication of an information signal from the fixed network communication unit **200** to the subscriber communication unit **202** will be described below. An information signal **212** is input to the base site controller **210** of the fixed network communication unit **200**. The base site controller **210** may perform several other operations in conjunction with communicating the information signal **212** besides providing cryptographic protection. These other operations may include but not limited to error protection encoding, voice encoding (vocoding), channel coding, modulation, and signal power amplification. However, these other operations may be performed in a number of different methods which are well known in the art. As such these other operations will not be discussed further in the following description so that the it may be focused specifically on a preferred embodiment cryptographic protection scheme of the present invention.

Once the information signal **212** is input to the base site controller **210**, the information signal is encrypted. The encryption

-5-

preferably is accomplished by providing the incoming information signal 212, 224 to an exclusive-or (XOR) gate 226 which combines it with a pseudo-random signal 218 from a PN generator 222. In the preferred embodiment, the pseudo-random signal 218 is a non-linear signal. The

5   method by which this non-linear pseudo-random signal 218 is generated will be discussed later in reference to FIG. 2. The output 228 of XOR gate 226 is an encrypted information signal. This encrypted information signal 228 may be further processed by the base site controller 210 prior to being operatively coupled through a signal

10   transmission line to antenna 206 for subsequent transmission over radio communication channel 204. It will be appreciated by those skilled in the art that the incoming information signal 224 may be combined according to some other function (i.e., not an XOR function) without departing from the scope and spirit of the present invention.

15   A subscriber unit 202 receives the encrypted information signal by an antenna and signal transmission line 208. The received encrypted information signal 208, 234 is input to an XOR gate 236 which combines it with a pseudo-random signal 238 from a PN generator 242 to decrypt the information signal. It will be appreciated

20   that PN generator 242 must be synchronized with PN generator 222 so that the PN signal 218, 238 output by both PN generators is in synch with the encrypted information signal. When the PN signal 238 is properly synchronized with the received encrypted information signal 234, the output 240 of the XOR gate 236 is a decrypted information

25   signal. This decrypted information signal 240 may be further processed by the subscriber unit 202 prior to being output from the subscriber unit 202 as information signal 250.

In a similar manner, an information signal may be communicated from the subscriber communication unit 202 to the fixed network

30   communication unit 200. An information signal 250 is input to a subscriber unit 202. The incoming information signal 250, 244 is encrypted with a non-linear pseudo-random signal 238 by an XOR gate 246. The encrypted information signal output 248 of the XOR gate 246 is coupled on a transmission line to an antenna 208 and transmitted on

35   a radio communication channel 204. The fixed network communication unit 200 receives encrypted information signal 206 and provides it to base site controller 210. Base site controller 210 combines the

received encrypted information signal **206, 214** with a non-linear
pseudo-random signal **218** by XOR gate **216** to decrypt the information
signal. The non-linear pseudo-random signal **218** is synchronized with
the non-linear pseudo-random signal **238** that was originally used to

5   encrypt the information signal. XOR gate **216** outputs a decrypted
information signal **220** which is then provided to the fixed network
through a coupler **212**.

Turning now to FIG. 2, a block diagram of a preferred
embodiment pseudo-random signal (i.e., bit sequence) generator **222**,

10   **242** to be used by either the subscriber unit **202** or the fixed network
communication unit **200** is shown. By way of example, a seven bit
pseudo-random bit sequence generator **222, 242** is described.
However, it will be appreciated by those skilled in the art that larger
pseudo-random bit sequence generators may be used in encrypting an

15   information signal to provide better cryptographic protection of the
information signal (i.e., it is more difficult to "break" or "crack" longer non-
linear sequences than shorter ones). In addition, the use of these larger
pseudo-random bit sequence generators does not depart from the
scope and spirit of the present invention.

20   The seven bit pseudo-random bit sequence generator **222, 242**
preferably is implemented as a feedback register that implements
several polynomial functions and as such includes a shift register **252**
for storing a predetermined number of bits (e.g., seven bits numbered D_0
through D_6). In addition, a first feedback circuit **254** is operatively

25   coupled to the shift register **252**. In the preferred embodiment, the first
feedback circuit implements a polynomial function x^7+x^3+1 by "tapping"
inputs for an XOR gate **254** from bits (i.e., D_3 and D_6) stored in the shift
register **252**. The output of XOR gate **254** determines a first input bit
260 which may be selectively input to a serial input of the shift register

30   **252**. A second feedback circuit **256** also is operatively coupled to the
shift register **252**. The second feedback circuit preferably implements a
polynomial function $x^7+x^4+x^3+x^2+1$ by "tapping" inputs for an XOR gate
256 from bits (i.e., D_2, D_3, D_4, and D_6) stored in the shift register **252**.
The output of XOR gate **256** determines a second input bit **262** which

35   may be selectively input to a serial input of the shift register **252**. The
first **260** and second **262** input bit are input to a feedback selection
controller **266** which outputs **268** one of the two input bits to the shift

-7-

register **252**. Feedback selection controller **266** deterministically
selects according to an algorithm a particular input bit (i.e., either input
bit **260** or **262**) to be provided to the shift register **252** such that a non-
linear pseudo random sequence may be produced by the shift register
5   **252** and output on serial output **218, 238**. In order to ensure that the
pseudo random sequence which is output **218, 238**, the pseudo
random bit sequence generator **222, 242** will need to be initialized and
clocked through several cycles to randomly mix the output sequence.
The minimal number of clock cycles required for pseudo random mixing
10   is N, where N is the length of the shift register **252** (in this example
seven clock cycles is required). In addition, to prevent susceptibility to
cryptographic attack (i.e., code breaking), the feedback selection
controller **266** must not select particular input bits from the same
feedback circuit **254** or **256** for more than 2N clock cycles, where N is
15   the length of the shift register **252**. By selecting input bits from different
feedback circuits more often, a cryptographic attacker is prevented from
using a linear equation solution attack. Finally, it will be appreciated by
those skilled in the art that more that two feedback circuits may be used
to further enhance the non-linearity of the pseudo-random sequence
20   **268** serially input to shift register **252**.

The feedback selection controller **266** preferably includes an
internal control mechanism which selects (i.e., switches between) the
particular input bit according to an algorithm based on an internal input
264. The internal input **264** consists of an output of a gate function **258**
25   of a plurality of "untapped" bits (e.g., an AND gate function of D_0 and
D_1) of the shift register **252**. If this internal control mechanism operates
according to this algorithm, the input bits provided to the shift register
252 in a sequence according to Table 1 as shown below.

-8-

Table 1

Register Stages	Control Bit	Switch	New Input Bit
1010101	1·0=0	up	$0\oplus1=1$
1101010	1·1=1	down	$0\oplus1\oplus0\oplus0=1$
1110101	1·1=1	up	$0\oplus1=1$
1111010	1·1=1	down	$1\oplus1\oplus0\oplus0=0$
0111101	0·1=0	down	$1\oplus1\oplus1\oplus1=0$
0011110	0·0=0	down	$1\oplus1\oplus1\oplus0=1$
1001111	1·0=0	down	$0\oplus1\oplus1\oplus1=1$
1100111	1·1=1	up	$0\oplus1=1$
1110011	1·1=1	down	$1\oplus0\oplus0\oplus1=0$
0111001	0·1=0	down	$1\oplus1\oplus0\oplus1=1$
⋮	⋮	⋮	⋮

It will be appreciated that another internal control mechanism may
5   be used (e.g., a parity bit of the shift register **252** or a function of a
plurality of any bits (i.e., "tapped" or "untapped") of the shift register
252). In addition, the feedback selection controller **266** may include an
external control mechanism which selects the particular input bit
according to an algorithm based on an external input. Examples of
10   external input include a linear feedback shift register output, a clock
initialization signal, and a cellular automaton. Cellular automaton
concepts were discussed in "Analysis of Cellular Automata Used as
Pseudorandom Pattern Generators" by Paul H. Bardell in a paper
presented at the 1990 International Test Conference. Further, the
15   feedback selection controller **266** may include a combination of an
internal and external control mechanism. Finally, the feedback selection
controller **266** may use an entirely different control mechanism which
selects the particular input bit by selecting a value from a lookup table
which is addressed by a plurality of bits of the shift register **252**.
20   The preferred embodiment of the present invention may be
summarized with reference to the subscriber communication unit **202** in
the following manner. A communication device for use in maintaining
secure communications through an encryption process between a
subscriber unit **202** and fixed network communication units **200** of a

serving communication system is provided. The transmitting portion of the communication unit includes a pseudo-random bit sequence generator **242** which generates a non-linear pseudo-random bit sequence **238**. The pseudo-random bit sequence generator **242**

5 includes a shift register **252** for storing a predetermined number of bits (i.e., D_0 through D_6). In addition, a first feedback device **254** is operatively coupled to the shift register **252**. The first feedback device **254** determines a first input bit **260** as a function of bits stored in the shift register **252**. Further, a second feedback device **256** is operatively

10 coupled to the shift register **252**. The second feedback device **256** determines a second input bit **262** as a function of bits stored in the shift register **252**. Finally, the pseudo-random bit sequence generator **242** includes a controller **266** operatively coupled to the shift register **252**, the first feedback device **254**, and the second feedback device **256**.

15 The controller **266** deterministically selects a particular input bit to be provided **268** to the shift register **252**. This particular input bit is either the first input bit **260** or the second input bit **262**.

The transmitting portion of the communication unit also includes an encrypting device **246**, operatively coupled to the pseudo-random bit

20 sequence generator **242**, which encrypts an input information signal **244, 250** as a function of the non-linear pseudo-random bit sequence **238**. A transmitter **208**, operatively coupled to the encrypting device **246**, transmits the encrypted information signal **248** over a communication channel **204**.

25 The receiving portion of the communication device includes a receiver **208** for receiving an encrypted information signal from a communication channel **204**. In addition, the receiving portion uses the same or at least a substantially similar pseudo-random bit sequence generator **242** as is used by the transmitting portion. This pseudo-

30 random bit sequence generator **238** generates a non-linear pseudo-random bit sequence **238**. Finally, a decrypting device **236**, operatively coupled to the receiver **208** and the pseudo-random bit sequence generator **238**, for decrypts the received encrypted information signal **234** as a function of the non-linear pseudo-random bit sequence **238**

35 into the information signal **240, 250**.

Although the invention has been described and illustrated with a certain degree of particularity, it is understood that the present

-10-

disclosure of embodiments has been made by way of example only and that numerous changes in the arrangement and combination of parts as well as steps may be resorted to by those skilled in the art without departing from the spirit and scope of the invention as claimed. For

5   example, the communication channel could alternatively be an electronic data bus, wireline, optical fiber link, satellite link, or any other type of communication channel.

-11-

Claims

What is claimed is:

5   1.   A pseudo-random bit sequence generator, comprising:

    (a)   shift register means for storing a predetermined number of bits;

    (b)   first feedback means, operatively coupled to the shift register means, for determining a first input bit as a function

10   of bits stored in the shift register means;

    (c)   second feedback means, operatively coupled to the shift register means, for determining a second input bit as a function of bits stored in the shift register means; and

    (d)   control means, operatively coupled to the shift register

15   means, the first feedback means, and the second feedback means, for deterministically selecting a particular input bit to be provided to the shift register means such that a non-linear pseudo random sequence may be produced by the shift register means, the particular input bit being selected

20   from the group consisting of the first input bit and the second input bit.

2.   The pseudo-random bit sequence generator of claim 1 wherein the control means comprises an external control mechanism

25   which selects the particular input bit according to an algorithm based on an external input, and the external input is selected from the group consisting of a linear feedback shift register output, a clock initialization signal, and a cellular automaton.

30   3.   The pseudo-random bit sequence generator of claim 1 wherein the control means comprises an internal control mechanism which selects the particular input bit according to an algorithm based on an internal input, and the internal input is selected from the group consisting of a parity bit of the shift register means, a

35   function of a plurality of bits of the shift register means, and a function of a plurality of untapped bits of the shift register means.

-12-

4.   The pseudo-random bit sequence generator of claim 1 wherein
        the control means comprises internal and external control
        mechanisms which selects the particular input bit according to an
        algorithm based on an internal input and an external input,
5   respectively.

5.   The pseudo-random bit sequence generator of claim 4 wherein:
        (a)   the algorithm comprises logically combining the internal
                input and the external input into a selection signal;
10   (b)   the internal input is selected from the group consisting of a
                parity bit of the shift register means, a function of a plurality
                of bits of the shift register means, and a function of a
                plurality of untapped bits and of the shift register means;
                and
15   (c)   the external input is selected from the group consisting of a
                linear feedback shift register output, a clock initialization
                signal, and a cellular automaton.

6.   The pseudo-random bit sequence generator of claim 1 the control
20   means comprises a mechanism for selecting the particular input
        bit according to an algorithm consisting of selecting a value from
        a lookup table which is addressed by a plurality of bits of the shift
        register means.

25 7. A communication device for use in maintaining secure
        communications through an encryption process between a
        subscriber unit and fixed network communication units of a
        serving communication system, comprising:
        (a)   a pseudo-random bit sequence generator means for
30   generating a non-linear pseudo-random bit sequence, the
                pseudo-random bit sequence generator means
                comprising:
                (i)   shift register means for storing a predetermined
                        number of bits;
35   (ii)   first feedback means, operatively coupled to the shift
                        register means, for determining a first input bit as a
                        function of bits stored in the shift register means;

-13-

(iii)   second feedback means, operatively coupled to the shift register means, for determining a second input bit as a function of bits stored in the shift register means; and

5   (iv)   control means, operatively coupled to the shift register means, the first feedback means, and the second feedback means, for deterministically selecting a particular input bit to be provided to the shift register means, the particular input bit being

10   selected from the group consisting of the first input bit and the second input bit;

(b)   encrypting means, operatively coupled to the pseudo-random bit sequence generator means, for encrypting an input information signal as a function of the non-linear

15   pseudo-random bit sequence; and

(c)   transmitting means, operatively coupled to the encrypting means, for transmitting the encrypted information signal over a communication channel.

20   8.   A communication device for use in maintaining secure communications through an encryption process between a subscriber unit and fixed network communication units of a serving communication system, comprising:

(a)   receiving means for receiving an encrypted information

25   signal from a communication channel.

(b)   a pseudo-random bit sequence generator means for generating a non-linear pseudo-random bit sequence, the pseudo-random bit sequence generator means comprising:

30   (i)   shift register means for storing a predetermined number of bits;

(ii)   first feedback means, operatively coupled to the shift register means, for determining a first input bit as a function of bits stored in the shift register means;

35   (iii)   second feedback means, operatively coupled to the shift register means, for determining a second input

bit as a function of bits stored in the shift register means; and

(iv) control means, operatively coupled to the shift register means, the first feedback means, and the second feedback means, for deterministically selecting a particular input bit to be provided to the shift register means, the particular input bit being selected from the group consisting of the first input bit and the second input bit; and

(c) decrypting means, operatively coupled to the receiving means and the pseudo-random bit sequence generator means, for decrypting the received encrypted information signal as a function of the non-linear pseudo-random bit sequence.

9. A method for generating a pseudo-random bit sequence, comprising:

(a) determining a first input bit as a function of bits stored in a shift register in accordance with a first feedback algorithm;

(b) determining a second input bit as a function of bits stored in the shift register in accordance with a second feedback algorithm; and

(c) deterministically selecting a particular input bit to be provided to the shift register such that a non-linear pseudo random sequence may be produced by the shift register, the particular input bit being selected from the group consisting of the first input bit and the second input bit.

10. The method of claim 9 wherein the step of deterministically selecting a particular input bit is based on an input selected from the group consisting of:

(a) an external input selected from the group consisting of a linear feedback shift register output, a clock initialization signal, and a cellular automaton;

(b) an internal input selected from the group consisting of a parity bit of the shift register, a function of a plurality of bits

-15-

of the shift register, and a function of a plurality of untapped
bits of the shift register;

(c)   a selection signal derived from logically combining an
internal input and an external input, the internal input being
5   selected from the group consisting of a parity bit of the shift
register, a function of a plurality of bits of the shift register,
and a function of a plurality of untapped bits and of the shift
register, and the external input being selected from the
group consisting of a linear feedback shift register output, a
10   clock initialization signal, and a cellular automaton; and

(d)   a value from an lookup table which is addressed by a
plurality of bits of the shift register.
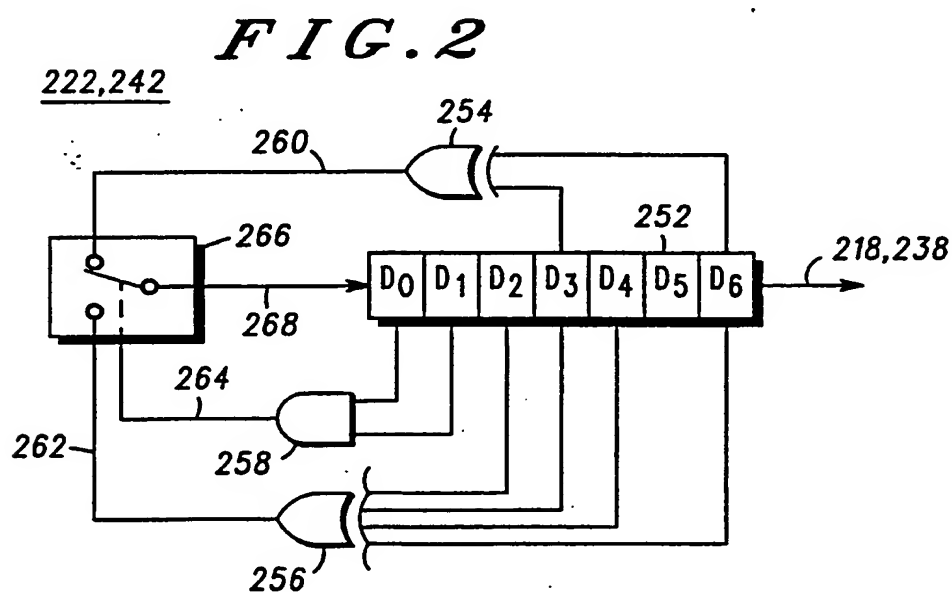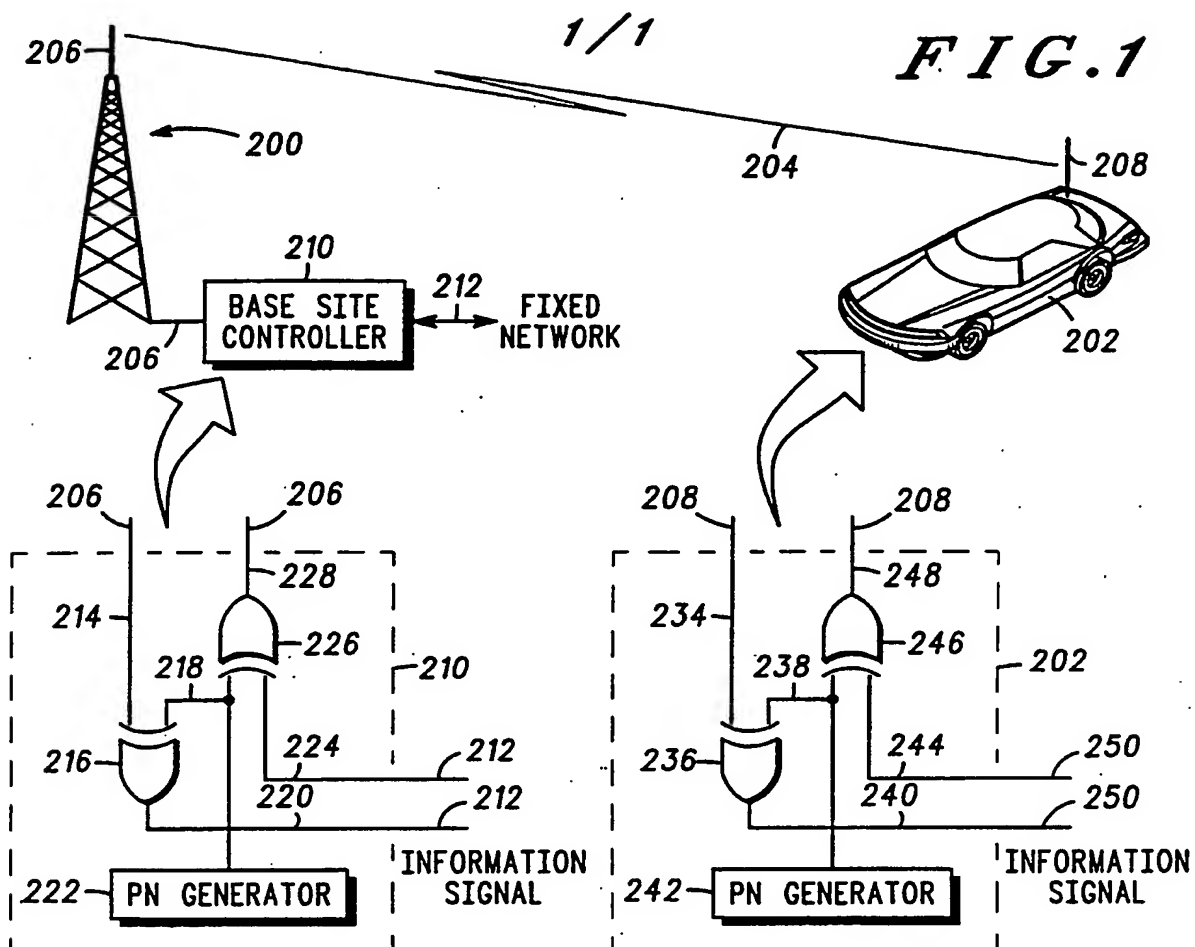
1/1

FIG.1

FIG.2

INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER

IPC(5) :G06F 1/02
US CL :380/46

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/46
380/9, 49, 50; 331/78; 364/717

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US, A, 3,728,533 (MATTHEWS) 17 APRIL 1973.	1-10
A	US, A, 4,590,601 (BEEMAN) 20 MAY 1986.	1-10
A	US, A, 4,611,183 (PIOSENKA ET AL) 08 SEPTEMBER 1986.	1-10
A	US, A, 4,890,252 (WANG) 26 DECEMBER 1989.	1-10

☐ Further documents are listed in the continuation of Box C.   ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be part of particular relevance		
"E"	earlier document published on or after the international filing date	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed	"&"	document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 AUGUST 1994	**SEP 02 1994**
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231	Authorized officer BERNARR EARL GREGORY
Facsimile No. (703) 305-3230	Telephone No. (703) 308-0479

Form PCT/ISA/210 (second sheet)(July 1992)*